UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/065,291	10/01/2002	Xiao-Qin Yu	IACP0019USA	5715

27765 7590 04/07/2006

NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER	
TO, BAOTRAN N	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/065,291	YU ET AL.	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 October 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/01/2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 are pending in the application.

Drawings

The drawings are objected to because the element 74 "ideutifying module" in Figure 3 should be ---identifying module. Appropriate correction is required. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

2. Claim 3 is objected to because of the following informalities: the phrase "Rivest Shamir Asleman (RSA) algorithm" in line 2 should be Rivest Shamir Adelman (RSA) algorithm. Appropriate correction is required.

Claim 14 is objected to because of the following informalities: the phrase "the forth algorithm" in line 14 should be the fourth algorithm. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (U.S. Patent 6,198,824 B1) hereinafter Shambroom in view of Eschelbeck et al. (U.S. Patent 6,611,869 B1) hereinafter Eschelbeck.

Regarding Claim 1, Shambroom discloses a method for applying for crypto-keys from a network system, the network system comprising at least a first user client, an access point having an identifying module and a user list, and a certificate server, the access point being used to receive a certificate packet from the first user client and to

utilize the identifying module to verify the certificate packet according to the user list so as to generate a verification signal, the certificate server being used to generate a pair of distinct crypto-keys according to the verification signal and a first algorithm (see Figure 4), the method comprising:

utilizing the first user client (client 200) to generating the certificate packet (col. 7, lines 40-55);

utilizing the access point (network server 300) to receive the certificate packet (col. 7, lines 45-50);

utilizing the identifying module to verify the certificate packet according to the user list so as to generate the verification signal (col. 2, lines 30-35 and col. 8, lines 16-23), and

transmitting the verification signal to the certificate server (col. 8, lines 15-20);

controlling the certificate server to transmit the pair of crypto-keys to the access point (Figure 5A, element 608 and col. 9, lines 28-32); and

controlling the access point to transmit the pair of crypto-keys to the first client (col. 10, lines 55-65).

Shambroom does not explicitly disclose "utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm."

However, Eschelbeck expressly discloses utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm (col. 6, lines 30-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Eschelbeck's invention with Shambroom to provide utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm. One of ordinary skill in the art would have been motivated to allow for enhancing the security of a message sent through a network (Abstract of Shambroom).

Regarding Claim 2, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Shambroom discloses wherein the certificate packet comprises a user name and a password (col. 8, lines 15-20).

Regarding Claim 3, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Eschelbeck discloses wherein the first algorithm is a Rivest Shamir Asleman (RSA) algorithm (col. 2 lines 35-40).

Regarding Claim 4, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Eschelbeck discloses wherein the first algorithm is a digital signature algorithm (DSA) (col. 5, lines 50-65).

Regarding Claim 5, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Eschelbeck discloses wherein the pair of crypto-keys is a public key and a private key (col. 6, lines 30-35).

Regarding Claim 6, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Shambroom discloses wherein the network system further comprises at least a second user client communicating with the access point, and the first user client comprises a first encryption module for encrypting a plain text into a ciphered text according to a second algorithm and a first key of the pair of crypto-keys, the second user client comprises a second decryption module for decrypting the ciphered text into the plain text according to a third algorithm and a second key of the pair of crypto-keys (Figure 3), the method further comprising:

transmitting the second key from the first user client through the access point to the second user client (destination server) (Figure 1);

utilizing the first encryption module to encrypt the plain text into the cipher text according to the second algorithm and the first key (col. 7, lines 30-35);

transmitting the ciphered text from the first user client through the access point to the second user client (col. 7, lines 40-45); and

utilizing the second decryption module to decrypt the ciphered text according to the third algorithm and the second key (col. 7, lines 40-45).

Regarding Claim 7, Shambroom and Eschelbeck disclose the limitations of Claim 6 above. Furthermore, Eschelbeck discloses wherein the second algorithm and third algorithm are associated with the first algorithm (col. 2, lines 35-40).

Regarding Claim 8, Shambroom and Eschelbeck disclose the limitations of Claim 6 above. Furthermore, Shambroom discloses wherein the first user client further-comprises a first decryption module for decrypting the ciphered text into the plain text according to the third algorithm and the first key, and the second user client further comprises a second encryption module for encrypting the plain text into the ciphered text according to the second algorithm and the second key (Figure 3), the method further comprising:

utilizing the second encryption module to encrypt the plain text into the ciphered text according to the second algorithm and the second key (col. 9, lines 10-30);

transmitting the from the second user client through the access point to the first user client (col. 9, lines 10-15); and

utilizing the first decryption module to decrypt the ciphered text according to the third algorithm and the first key (col. 9, lines 40-50).

4. Claims 9-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom and Eschelbeck as applied to claim 1 above, and further in view of Sandhu et al. (U.S. Patent 7,017,041 B2) hereinafter Sandhu.

Regarding Claim 9, Shambroom and Eschelbeck disclose the limitations of Claim 6 above. Furthermore, Shambroom discloses wherein the network system further comprises at least a second user client communicating with the access point, and the first user client comprises a first encryption module for encrypting numbers according to a second algorithm and a first key of the pair of crypto-keys, the second user client comprises a second decryption module for decrypting numbers according to a third algorithm and a second key of the pair of crypto-keys (Figure 3 and , the method further comprising:

transmitting the second key from the first user client through the access point to the second user client (figure 2);

controlling the first user client to convert a plain text into a first value according to a fourth algorithm (col. 7, lines 25-50);

utilizing the first encryption module to encrypt the first value according to the second algorithm and the first key (col. 8, lines 15-35);

transmitting the and the encrypted first value from the first user client through the access point to the second user client (col. 10, lines 35-50);

utilizing the second decryption module to decrypt the encrypted first value according to the third algorithm and the second key (col. 9, lines 30-40);

Shambroom and Eschelbeck do not disclose "controlling the second user client to convert the plain text into a second value according to the fourth algorithm; and comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client."

However, Sandhu expressly discloses controlling the second user client to convert the plain text into a second value according to the fourth algorithm; and comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client (col. 1, lines 50-67 through col. 2, lines 1-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined Shambroom's invention and Eschelbeck's invention with Sandhu to include controlling the second user client to convert the plain text into a second value according to the fourth algorithm; and comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client. One of ordinary skill in the art would have been motivated to allow for enhancing the security of a message sent through a network (Abstract of Shambroom).

Regarding Claim 10, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the fourth algorithm is a message digest 2 (MD2) algorithm (col. 2, lines 15-25).

Regarding Claim 11, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the fourth algorithm is a message digest 5 (MD5) algorithm (col. 2, lines 15-25).

Regarding Claim 12, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the fourth algorithm is a secure Hash algorithm (SHA) (col. 2, lines 15-25).

Regarding Claim 13, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the second algorithm and third algorithm are associated with the first algorithm (col. 3, lines 15-25).

Regarding Claim 14, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the first user client further comprises a first decryption module for decrypting numbers according to the third algorithm and the first key, and the second user client further comprises a second encryption module for encrypting numbers according to the second algorithm and the second key (Figure 4), the method further comprising:

controlling the second user client to convert the plain text to the first value according to the fourth algorithm (col. 20, lines 15-45);

utilizing the second encryption module to encrypt the first value according to the second algorithm and the second key (col. 8, lines 45-65);

transmitting the and the encrypted first value from the second user client through the access point to the first user client (col. 7, lines 20-45);

utilizing the first decryption module to decrypt the encrypted first value according to the third algorithm and the first key (col. 6, lines 15-25);

controlling the first user client to convert the forth algorithm (col. 1, lines 50-67 through col. 2, lines 1-25); and

comparing the second value with the decrypted first value to verify the plain text transmitted from the second user client to the first user client (col. 2, lines 1-25).

Prior Art

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Stringer et al. (U.S. Patent 6,971,017 B2)

Kadyk et al. (U.S. Patent 6,996,841 B2)

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

HOSUK SONG
PRIMARY EXAMINER

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

03/31/2006
Baotran To